## Compliance by design

Goudsmit, Jeroen; van der Valk, Bauk

***published in***
Tijdschrift voor Compliance
2021

***document version***
Publisher's PDF, also known as Version of record

# Compliance by design

## *Bouwen aan een duurzaam compliant organisatie*

*drs. B. van der Valk MSc en dr. J.P. Goudsmit*[1]

**Compliant zijn met de veelheid aan externe en interne normen is complex. Wij stellen dat dit alleen mogelijk is indien deze normen volledig geïntegreerd zijn in de bedrijfsprocessen, zodat bij correcte uitvoering van deze processen voldaan is aan de gestelde normen. Dit vereist een volledig integriteitsbeeld: een overzicht van de normen, de processen waarin deze van toepassing zijn, en de vereisten waarmee de normen geborgd worden. Met deze basis kan gebouwd worden aan een duurzaam compliant organisatie door zowel de eerste als de tweede lijn.**

Compliance is veeleisend. Elke organisatie van enig formaat is onderhevig aan een veelheid van wetten en regelgeving. Daarnaast heeft de organisatie intern beleid gericht op het uitvoeren van de missie conform strategie – handelend naar de gekozen waarden en binnen de risicotolerantie. Het in kaart brengen van al deze normen is geen geringe opgave. Wetten en regels kunnen ambigu zijn, elkaar tegenspreken, en veranderen geregeld. En: dit alles moet altijd, en altijd goed.

Compliance begint met gedrag: de *tone at the top* en de juiste attitude van medewerkers.[2] Zij moeten bekend zijn met de van toepassing zijnde werkinstructies, interne procedures, waarden en relevante wet- en regelgeving. Dat is nogal wat om in gedachten te houden. Daarom is een invulling van compliance die uitsluitend leunt op gedrag een fragiel uitgangspunt. Een organisatie moet kunnen uitleggen aan interne en externe toezichthouders hoe deze heeft gekozen zich te conformeren aan geldende wet- en regelgeving. Wanneer binnen de organisatie voor verschillende interpretaties van dezelfde termen of normen is gekozen, dan bemoeilijkt dit een coherente verantwoording aan deze toezichthouders. Zeker wanneer daarnaast ook nog eens in vergelijkbare situaties sprake was van onvergelijkbare risicotoleranties ten opzichte van non-compliance. Ook maakt het er de situatie niet gemakkelijker op als ketenpartners sterk afwijkende keuzes maken.

Het voldoen aan al deze normen is inherent complex en vereist veel inzicht in zowel de regelgeving als in de bedrijfsprocessen en de ondersteunende informatiesystemen.
In dit artikel kijken we naar de processen van een organisatie en de rol die deze kunnen spelen bij het bevorderen van compliance. We stellen dat als een organisatie duurzaam compliant wil zijn, gegarandeerd moet kunnen worden dat bedrijfsprocessen op een samenhangende wijze invulling geven aan de geldende normen. Hieronder geven we aan wat we verstaan onder deze normen, hoe we de koppeling zien met bedrijfsprocessen, en wat de uitdagingen zijn bij een coherente borging van deze normen in de bedrijfsprocessen.
In sectie 2 beginnen we met de scope van compliance. Compliance begint met de normen waar de organisatie zich kiest aan te conformeren, en vertaalt zich via een aantal (al dan niet bewuste) keuzes naar wat de organisatie bereid is te doen en eindigt met hoe deze hier concreet invulling aan geeft. Normen kunnen komen vanuit wetgeving, verwachtingen van toezichthouders, maar vanzelfsprekend ook uit de strategie die de organisatie zelf gekozen heeft. De gedachte achter *compliance by design* zit in het van de grond af aan het 'wat' van de wet- en regelgeving onderdeel maken van de processen die het 'hoe' invullen.
Vervolgens duiken we in sectie 3 de bedrijfsprocessen in. Volwassen processen zijn de basis van een gezonde organisatie en bieden de kaders voor een beheerste bedrijfsvoering. Organisaties polijsten hun processen om zo efficiënt mogelijk functionele vereisten te verwezenlijken: bijdragen aan een competitieve portfolio van producten en diensten. Compliance vereisten vormen een tegendruk op deze functionele eisen: zij stellen eisen om te voldoen aan wet- en regelgeving, dit kan strijdig zijn met de effectiviteit en efficiëntie van processen. Het vinden van een evenwicht tussen de functionele en niet-functionele (compliance) eisen aan bedrijfsprocessen is niet eenvoudig.

1. Bauk van der Valk is zelfstandig adviseur over *governance* en compliance vraagstukken in relatie tot ICT, en Jeroen Goudsmit doceert Kwantitatief Integriteitsmanagement aan de Vrije Universiteit Amsterdam en is tevens compliance officer ter bestrijding van witwassen, terrorismefinanciering en sanctie-overtredingen bij de Rabobank.
2. Bleker-van Eyk, S., & Janssen, F. (2020). Conduct risk, de heilige graal van compliance. *Tijdschrift Voor Compliance*, 5, 275–284.

We komen tot de kern van *compliance by design* in sectie 4. We beschrijven de drie uitdagingen in het samenspel tussen functionele en compliance vereisten aan processen. We pleiten voor het duidelijk beleggen van de eindverantwoordelijkheid voor het opstellen van compliance vereisten in de eerste lijn. Door dit onderdeel te maken van de gangbare *governance* voor het vernieuwen van bedrijfsprocessen wordt gaandeweg gebouwd aan de duurzaam compliant organisatie.

## 1. Kennen van normen

Compliance begint met het kennen van de normen waaraan voldaan moeten worden. Deze kunnen zowel voortvloeien uit interne keuzes van de organisatie qua waarden en strategie, als extern opgelegd zijn vanuit wet- en regelgeving.[3] Merk hierbij op dat bij een enge lezing dit reeds alle van toepassing zijnde wetgeving omvat, zoals algemeen geldende wetten als arbeids-, contractrecht, omgevingswet, en de algemene verordening gegevensbescherming. Iets breder gezien vallen hieronder ook extern bepaalde normen zoals vastgelegd in branche-specifieke regelgeving (denk aan opleidingseisen en tucht- en klachtrecht), contracten met leveranciers en afnemers (zoals betaaltermijnen en *service level agreements*), en zelfs vrijwillige verbintenissen met maatschappelijke organisaties (bijvoorbeeld inzake keurmerken of maatschappelijk verantwoord ondernemen). De bovengenoemde externe normen gaan verder dan wat puur juridisch bindend is, en omvatten alle standaarden en verwachtingen aangaande integriteit en betamelijk handelen.[4]

Bovengenoemde normen kunnen in verschillende vormen gepresenteerd worden. Sommigen zijn sterk 'imperatief' en vertellen 'hoe' iets gedaan dient te worden. Denk hierbij aan de expliciete normen gangbaar in de luchtvaarsector of farmacie, waar vanuit toezichthouders op basis van hard geleerde lessen omschreven wordt hoe iets gedaan dient te worden. [5] Andere zijn 'declaratief' en omschrijven 'wat' er gedaan dient te worden, doorgaans algemene principes die risico-gebaseerd toegepast dienen te worden (*principle based).*[6]

Vervolgens is het aan de organisatie om positie in te nemen. Er moet beschreven worden wat de consequenties van deze algemene normen zijn in termen van concrete compliance vereisten aan de organisatie. De complexiteit van de vertaling van normen naar vereisten wordt bepaald door de mate van ambiguïteit in normen en hun onderlinge wrijving. Een sterk imperatieve norm is immers eenvoudiger een-op-een te vertalen naar een concrete vereiste dan een declaratief omschreven principe dat naar eigen inzicht risico gebaseerd toegepast dient te worden. Tevens kan wet- en regelgeving met elkaar op gespannen voet staan, wat een samenhangende invulling hiervan bemoeilijkt. Denk hier aan de Europese gegevensbeschermingswetgeving en de zorgplicht van financiële instellingen: de zorgplicht kan minder uitgevoerd worden naar gelang het principe van data-minimalisatie stringenter toegepast wordt.[7]

Ten slotte dient geborgd te worden dat de gekozen positie consistent gehandhaafd wordt, wat door drie perspectieven bereikt kan worden. Het eerste perspectief is 'correctief': niet-compliant gedrag achteraf herstellen wanneer het bekend wordt. Daarnaast kan men 'opsporend' te werk gaan, door actief en structureel niet-compliant gedrag handmatig of automatisch op te sporen. Het 'preventieve' perspectief is gericht op het zo inrichten van de organisatie dat niet-compliant gedrag zo moeilijk mogelijk gemaakt wordt. Het zorgen voor een bedrijfscultuur waarin compliant gedrag in alle lagen van de organisatie centraal staat kan gezien worden als een onderdeel van dit preventieve perspectief. *Compliance by design* ligt in dit verlengde.[8]

## 2. Volwassen processen als basis voor compliance

Het verankeren van duurzame compliance vereist dat bedrijfsprocessen zodanig zijn ingericht dat zij bij correcte uitvoering voldoen aan de gestelde compliance vereisten. De eindverantwoordelijkheid voor de opzet van deze processen en de verankering van hun werking in de organisatie ligt bij het senior management: de eerste lijn.[9] Zij moeten er

3. Bleker-van Eyk, S., & Houben, R. (Eds.). (2017). Handbook of Compliance & Integrity Management: Theory and Practice. *Kluwer Law International B.V.*
4. Basel Committee on Banking Supervision. (2005). Compliance and the compliance function in banks. *Bank for International Settlements.* https://www.bis.org/publ/bcbs113.htm
5. In de luchtvaart is het opvolgen van compliance eisen zo belangrijk dat er een taalopleiding is die borgt dat nietnative speakers in staat zijn om te voldoen aan de compliance vereisten: Emery, H., Roberts, A., Goodman, R., & Harrison, L. (2008). Aviation English: for ICAO compliance. Oxford: Macmillan
6. Zie bijvoorbeeld de Wet ter voorkoming van witwassen en financieren van terrorisme, https://wetten.overheid.nl/BWBR0024282/2020-10-15
7. European Union Agency for Fundamental Rights, & Council of Europe. (2018). Handbook on European data protection law (2018 edition). Publications Office of the European Union. https://doi.org/10.2811/343461
8. Sadiq, S., & Governatori, G. (2015). Managing Regulatory Compliance in Business Processes BT - Handbook on Business Process Management 2: Strategic Alignment, Governance, People and Culture (J. vom Brocke & M. Rosemann (Eds.); pp. 265–288). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-45103-4_11
9. Merk op dat deze de vormgeving van deze processen ingevuld kan worden met behulp van staffuncties of externe adviseurs, maar de eindverantwoordelijkheid blijft onverminderd bij eerstelijns senior management. Immers wordt niet verwacht dat senior management zelf processen programmeert in IT-systemen, maar ze draagt hier wel de eindverantwoordelijkheid voor. Zie voetnoot 3 (BCBS 113), principe 2.

'preventief' voor zorgen dat wordt gewerkt conform de normen zoals vastgelegd in wet- en regelgeving, 'opsporend' normoverschrijdingen monitoren en hierop 'correctief' optreden.

Procesmatig werken is een voorwaarde om op voorspelbare wijze een competitieve portfolio van producten en diensten aan te kunnen bieden.[10] Producten en diensten worden voortgebracht door bedrijfsprocessen die zijn ingericht om functionele vereisten effectief en efficiënt te realiseren. Deze functionele vereisten geven een ondubbelzinnige omschrijving van de manier waarop een product of dienst wordt geleverd. Zo wordt, wanneer je tankt bij een zelfservicestation, eerst gecheckt of je rekeningcourant voldoende saldo heeft; zonder deze voorwaarde zou de dienst een stuk minder levensvatbaar zijn.
Organisaties hanteren doorgaans een *plan-do-check-act* (PDCA) cyclus om processen te ontwerpen, in te voeren, te toetsen en waar nodig te herijken. Voor financiële ondernemingen is het hebben van een procedure om nieuwe producten of diensten beheerst te introduceren zelfs een uitdrukkelijke vereisten.[11]
Methoden als *Lean Six Sigma* richten zich op het inrichten van processen die de functionele vereisten zonder verspilling en optimale doorlooptijden realiseren.[12] Deze methoden zijn er op gericht op bedrijfsprocessen zo competitief mogelijk te maken.
Op het eerste gezicht lijkt het toevoegen van compliance vereisten op een uitbreiding van deze functionele vereisten. Immers bepalen compliance vereisten mede de vorm van een proces, net zoals de functionele vereisten dat doen. Niettemin herkennen we twee fundamentele verschillen tussen deze vereisten, namelijk hun doel en levenscyclus.

Het doel van functionele vereisten is het voortbrengen van competitieve producten en diensten, terwijl het doel van compliance vereisten is om te conformeren aan interne of externe normen. Deze compliance vereisten kunnen leiden tot hogere kosten en complexere processen. Klassieke voorbeelden zijn functiescheiding en het vier-ogen-principe.[13] Deze methoden om controle op geld en goederenstromen te borgen in de procesuitvoering vragen extra activiteiten en betrokkenheid van meerdere personen, met als resultaat kostenverhoging en mogelijke doorlooptijdverlenging. Toch worden ze consequent toegepast, omdat ervaring geleerd heeft dat deze maatregelen zorgen voor een betere beheersing en zodoende problemen voorkomen.

Het ongezuiverd lozen van afvalwater is eenvoudiger en goedkoper dan het eerst zuiveren en ook te kunnen aantonen dat het water is gezuiverd voordat het geloosd is. De AVG staat niet toe dat persoonsgegevens zondermeer worden gebruikt voor het testen van informatiesystemen, echter: het anonimiseren of pseudonimiseren van gegevens is kostbaar en maakt het testen van ketens van informatiesystemen complex. De norm om gezuiverd te lozen en de norm voor data-minimalisatie maakt dat de organisatie extra investeringen moet doen en de processen complexer moet maken om de *licence to operate* te behouden. Dergelijke normen kunnen extern en juridisch bindend opgelegd zijn, maar kunnen ook ontstaan vanuit interne overtuigingen en waarden.

De levenscyclus van functionele vereisten heeft organisaties zelf in de hand. Dit betekent dat de organisatie zelf kan kiezen hoe en met welke tijdslijnen de *plan-do-check-act* cyclus doorlopen wordt om functionele vereisten te implementeren in bedrijfsprocessen. Dit in contrast met compliance vereisten, die kunnen ontstaan uit extern opgelegde normen waarvan de levenscyclus buiten de invloedssfeer van de organisatie kan liggen. De resulterende tijdslijnen op het doorlopen van de PDCA-cyclus kunnen dwingend zijn en zijn dikwijls uitdagend om te halen.
Een recent voorbeeld van een extern dwingend opgelegde norm betreft de maatregelen die voorgeschreven zijn in het kader van de coronapandemie. Verkoop van alcohol werd verboden na 20.00 uur. Voor de bezorgdiensten van supermarkten betekende dit dat leveringen na dit tijdstip geen alcoholhoudende dranken mochten bevatten.[14] Dit leidt tot een aanpassing van logistieke processen, aanvullende communicatie met klanten, wellicht aanpassing van de bezorgschema's en extra *controls* op de uitvoering. Dit alles leidt niet alleen tot hogere kosten en complexere processen, maar kan ook nog tot vermindering van de omzet leiden. De compliance vereisten zijn niet aanvullend op de functionele vereisten, maar concurrerend.

Om aan interne en externe toezichthouders te kunnen verantwoorden dat voldaan wordt aan de compliance vereisten is het noodzakelijk dat deze door de organisatie en de eventuele ketenpartners op coherente wijze worden nageleefd en dat dit door meetbare *controls* kan worden aangetoond. Dit vraagt om een beheerste uitvoering van bedrijfsprocessen. Processen zijn zoveel mogelijk gestandaardiseerd en waar mogelijk geautomatiseerd. In termen van procesvolwassenheid: processen zijn gedocumenteerd

10. Information Systems Audit and Control Association. (2018). *COBIT 2019 Framework: Introduction and Methodology*. https://www.isaca.org/
11. Zie Basel Committee on Banking Supervision. (2011). *Principles for the Sound Management of Operational Risk*. Bank for International Settlements. https://www.bis.org/publ/bcbs195.htm en Artikel32BesluitGedragstoezichtfinanciëleondernemingenWft.
12. Zie bijvoorbeeld *International Association for Six Sigma Certification*, https://iassc.org
13. Zie: Starreveld, R. W., H. B. De Mare, en E. J. Joëls. "Bestuurlijke informatieverzorging, deel 1: Algemene Grondslagen." Stenfert Kroese Groningen/Houten (2002).
14. Stil, H. (2020, Oktober 14). Websupers tegen het alcoholverbod na 20.00 uur: 'Dit is eigenlijk niet werkbaar.' *Het Parool*. https://www.parool.nl/amsterdam/websupers-tegen-het-alcoholverbod-na-20-00-uur-dit-is-eigenlijk-niet-werkbaar~b3d10d61/

en geïntegreerd over de organisatie en de eventuele ketenpartners.[15] De uitvoering ervan wordt gemonitord aan de hand van relevante *controls*. Dus ook voor de compliance eisen zijn meetbare afspraken gemaakt waar medewerkers en management aan moeten voldoen.
Hierbij moet een evenwicht worden gevonden tussen de functionele en de compliance vereisten binnen de risico-tolerantie van de organisatie voor compliance risico. Het bepalen van dit evenwicht is de verantwoordelijkheid van senior management. Het is zaak dat deze verantwoordelijkheid bewust genomen wordt. Om bij het voornoemde voorbeeld over de verkoop van alcohol aan te sluiten: als gevolg van deze nieuwe regelgeving zullen de kosten voor de supermarkten en bezorgdiensten omhooggaan en het is denkbaar dat de omzet daalt en daarmee de dienst minder competitief is. Senior management moet zich bewust zijn van deze gevolgen, zodat hier in de verdere bedrijfsvoering rekening mee gehouden kan worden.[16]

Op deze manier leidt *compliance by design* tot vermindering van de vrijheid van medewerkers en management om naar eigen inzicht hun werk uit te voeren. Immers wordt de gelegenheid om naar eigen inzicht keuzes te maken verminderd. Deze beperking van autonomie kan als ongewenst worden ervaren. Anderzijds vergroot *compliance by design* de mogelijkheid om de compliance vereisten geautomatiseerd te vervullen. Het bedrijfsproces kan deels door middel van ICT-ondersteuning worden gerealiseerd, waardoor minder repeterende werkzaamheden overblijven. Niettemin is het zaak om oog te houden voor de eisen van compliance en de regelruimte die nodig is om werk voldoende autonoom uit te kunnen voeren.[17] Belangrijk is hierin om alle betrokkenen te blijven informeren over nut en noodzaak van de gekozen werkwijze, en autonomie te laten bestaan binnen de mogelijkheden van compliance en effectiviteit van bedrijfsprocessen.

## 3. Architectuur van goed gedrag

Het integreren van compliance vereisten in de bedrijfsprocessen vraagt om een centrale en integrale sturing. We schetsen een manier om hier inrichting aan te geven binnen het raamwerk van COBIT2019.[18] Dit start met inzicht in de compliance vereisten, hoe deze door de organisatie (preventief) worden toegepast en in welke bedrijfsprocessen deze worden toegepast. Aanvullend kan (opsporend) gemonitord worden of in passende mate voldaan wordt aan de compliance vereisten, zodat (correctief) aanvullende maatregelen tijdig kunnen worden genomen. Hiervoor moet aan een drietal randvoorwaarden zijn voldaan.

Ten eerste moet een overzicht van geldende normen zoals omschreven in sectie 2 centraal vastgelegd zijn. Dit betreft wet- en regelgeving die met de producten en diensten van de organisatie te maken hebben,[19] maar ook wet- en regelgeving voor ondersteunende diensten. Zo heeft de Europese gegevensbeschermingswetgeving betrekking op alle persoonsgegevens, dus ook die van medewerkers of leveranciers. Naast externe verplichtingen kan een organisatie ook kiezen voor vrijwillige normen, bijvoorbeeld Fairtrade of de verbintenis met een beroepsorganisatie (zoals BOVAG) die aanvullende normen opleggen aan de bedrijfsvoering. De eindverantwoordelijkheid voor dit overzicht ligt bij het bestuur van de organisatie, en de compliance functie kan de verantwoordelijkheid nemen om dit overzicht te onderhouden.

Ten tweede moeten de bedrijfsprocessen voldoende volwassen zijn zoals besproken in sectie 3. Dit betekent dat de functionele vereisten afgedekt zijn in formeel vastgelegde processen. Ook moeten medewerkers voldoende kennis hebben zodat zij de processen conform deze vastlegging kunnen uitvoeren. De processen worden gemonitord aan de hand van *controls* op basis waarvan passende bijsturing plaatsvindt. In procesvolwassenheidsmodellen betekent dit: 'beheerst en meetbaar'.[20]

Ten derde moeten de normen worden vertaald naar passende compliance vereisten in de formele omschrijving van bedrijfsprocessen. Dit betekent dat de normen, die doorgaans declaratief en *principle based* opgesteld zijn, vertaald moeten worden naar eenduidig uitlegbare instructies. Deze eenduidig uitlegbaarheid is een randvoorwaarde voor het standaardiseren en automatiseren van processen. Dit is geen eenvoudige opgave omdat hiervoor een goed begrip

15. Zie bijvoorbeeld De Nederlandsche Bank. (2019). *Good practice informatiebeveiliging 2019-2020*. https://www.toezicht.dnb.nl/3/50-203304.jsp
16. Een voorbeeld van waar rekening mee gehouden zal moeten worden zijn de prestatie-indicatoren in de organisatie. Doorgaans zullen managers beoordeeld worden aan de hand van prestatie-indicatoren die deels hun bijdrage aan het realiseren van een competitieve portfolio van producten en diensten reflecteert. Door de introductie van nieuwe compliance-vereisen wordt hun vermogen dit te realiseren tot zekere hoogte beperkt. De prestatie-indicatoren van de managers moeten hier op aangepast worden. Zij zijn niet verantwoordelijk voor de (financiële) gevolgen van een nieuwe of aangescherpte norm.
17. Regelruimte is de vrijheid die een medewerker heeft om een taak naar eigen inzicht uit te voeren.
18. Zie voetnoot 10.
19. Denk aan de Wft voor financiële dienstverlening, maar ook aan de HACCP voor voedselveiligheid en het BIG-register voor medische beroepen.
20. Zie ook De Nederlandsche Bank. (2019). *Good practice informatiebeveiliging 2019-2020*. https://www.toezicht.dnb.nl/3/50-203304.jsp

van zowel de normen, de inhoud van de bedrijfsprocessen en van de vorm van procesontwikkeling nodig is. Het is uitzonderlijk om dit in één persoon terug te vinden.

Daarnaast is het noodzakelijk dat de normen coherent geïnterpreteerd worden over de verschillende bedrijfsprocessen heen, rekening houdend met een uniforme tolerantie voor de aanverwante compliance risico's. Zo is bijvoorbeeld de tolerantie voor onrechtmatig raadplegen van persoonsgegevens van klanten doorgaans voor alle bedrijfsprocessen gelijk. Als een proces het erg gemakkelijk maakt om klantgegevens te raadplegen, moeten er dus naar proportie zwaardere compliance vereisten aan dit proces en de ondersteunende informatiesystemen opgelegd worden om binnen deze tolerantie te blijven.

Laten we dit toelichten aan de hand van een concreet voorbeeld. [21] Het proces voor het raadplegen van patiëntgegevens in een ziekenhuis dwingt af dat een medewerker eerst geauthentiseerd wordt, vervolgens bepaald wordt of deze betrokken is bij de directe zorgverlening aan de patiënt, om toegang tot de gegevens te verlenen. Het proces kan ook de mogelijkheid bieden zonder authenticatie patiëntgegevens te raadplegen, om invulling te geven aan de functionele vereiste dat in geval van acute zorg de medewerker de juiste gegevens snel moet kunnen raadplegen. Om het verhoogde risico op het onrechtmatig raadplegen binnen tolerantie te mitigeren moet in het proces afgedwongen worden dat deze raadplegingen frequent integraal gecontroleerd worden. Hiermee wordt een gepaste balans geslagen tussen de functionele- en compliance- vereisten die binnen de tolerantie voor normoverschrijdingen blijft.

Wanneer is voldaan aan bovengenoemde drie voorwaarden ontstaat een overkoepelend 'integriteitsbeeld': een overzicht van de normen, de processen waarin deze van toepassing zijn, en de vereisten waarmee de normen geborgd worden. Met deze basis kan gebouwd worden aan een duurzaam compliant organisatie door zowel de eerste als de tweede lijn. Doorsnedes van dit integriteitsbeeld zijn reeds aanwezig in menig organisatie. Zo is bijvoorbeeld de beveiligingsarchitectuur een integriteitsbeeld op informatiebeveiliging en data-architectuur een integriteitsbeeld op (persoons)gegevensbescherming.[22] Zodoende kun je denken over dit integriteitsbeeld als de architectuur voor alle compliance risico's tezamen.

Senior management is verantwoordelijk voor het effectief beheersen van compliance risico.[23] Wanneer een bedrijfsproces (her)ontworpen wordt, moet het integriteitsbeeld geactualiseerd worden. Eerst zal bepaald worden of nieuwe normen van toepassing zijn, omdat bijvoorbeeld bedrijfsactiviteiten uitgevoerd worden in een nieuwe markt of jurisdictie. Daarna zal bepaald worden welke wijzigingen in functionele vereisten noodzakelijk zijn om de dienst competitief aan te bieden. Ten slotte wordt bepaald of huidige of nieuwe normen, onder staande risicotolerantie, aanleiding geven tot wijzigingen in of toevoegingen aan de compliance vereisten.

Eventuele conflicten tussen bovengenoemde functionele en compliance vereisten moeten door de eerste lijn zelf beslecht worden. Hiervoor is een wisselwerking tussen de eigenaar van het proces (senior management) en de proces-ontwikkelaar onontbeerlijk. Van de procesontwerper kan verwacht worden dat deze meerdere scenario's uitwerkt waarin de vereisten tegen elkaar afgezet worden, elk met een eigen complexiteit, kosten, en mate van effectiviteit en efficiëntie.
Doorgaans wordt in het procesontwerp de rol van bedrijfsarchitect gekend. Deze functionaris is verantwoordelijk voor de samenhang en inrichting van processen. De bedrijfsarchitect is uitdrukkelijk niet de eigenaar van de processen, maar faciliteert de eigenaar en diens ontwikkelaars in de totstandkoming van een beoogd bedrijfsproces wat past in het grotere geheel van de organisatie. Er bestaan reeds bedrijfsarchitecten die zich gespecialiseerd hebben in de beveiligings-architectuur of data-architectuur. We zien een duidelijke rol voor de breder georiënteerde compliance-architect die de procesontwikkelaar en proceseigenaar bij kan staan in de vertaling van normen naar compliance vereisten en de toepassing binnen processen.

Uiteindelijk is het aan senior management om een afweging te maken tussen deze scenario's en de keuze te maken. In het meest extreme geval kan de conclusie zijn dat de vereisten niet te rijmen zijn, oftewel: het beoogde product of de dienst kan niet competitief binnen de gestelde normen aangeboden worden. Deze afweging zou als vereiste meegenomen kunnen worden in de gangbare *governance* voor het vernieuwen van bedrijfsprocessen, zoals het productontwikkelings- en beoordelingsproces.[24]

De compliance functie ziet onafhankelijk toe op de voorgestelde afweging van senior management en toetst deze tegen het integriteitsbeeld en reeds bestaande analyses van integriteitsrisico.[25] Merk

21. Dit is ook een duidelijke verwachting van de toezichthouder, zie: Autoriteit Persoonsgegevens. (2019). *Besluit tot het opleggen van een bestuurlijke boete en een last onder dwangsom.* https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_haga_-_ter_openbaarmaking.pdf
22. Zie bijvoorbeeld NORA: https://www.noraonline.nl/wiki/Beveiliging/Architectuuraanpak
23. Zie bijvoorbeeld principe 2 uit BCBS 113 aangehaald in voetnoot 4: "The bank's senior management is responsible for the effective management of the bank's compliance risk".
24. Zie voetnoot 11.
25. Zie bijvoorbeeld De Nederlandsche Bank. (2015). *De integriteitrisicoanalyse - meer waar dat moet, minder waar dat kan.* https://www.toezicht.dnb.nl/2/50-234066.jsp

op dat de compliance functie noch de compliance vereisten opstelt, noch de afweging tussen de compliance- en functionele vereisten maakt. Dit zijn primair verantwoordelijkheden binnen de eerste lijn. *Compliance by design* is dus, net als compliance in het algemeen, geen activiteit die enkel aan de compliance functie toebehoort.

## 4. Conclusie

Duurzaam beheerste compliance vereist een beheerste inrichting van bedrijfsprocessen waar compliance in de aanleg is meegenomen. In een dergelijke inrichting is elk bedrijfsproces ontwikkeld om te voldoen aan functionele vereisten teneinde een competitief product of dienst te leveren en aan compliance vereisten teneinde te conformeren aan geldende normen.

Het integreren van compliance vereisten in de bedrijfsprocessen vraagt om een centrale en integrale sturing welke leunt op een overkoepelend integriteitsbeeld: een overzicht van de normen, de processen waarin deze van toepassing zijn, en de vereisten waarmee de normen geborgd worden. Dit integriteitsbeeld vormt de architectuur van compliance die bewaakt kan worden door een of meerdere compliance architecten.

De vertaling van geldende nomen naar compliance vereisten moet coherent gebeuren op basis van een uniforme risico-tolerantie. De keuze in deze vertaling en de opvolgende invulling aan functionele- en compliance vereisten is aan de proceseigenaar, die hierin ondersteund kan worden door een gespecialiseerde compliance architect. Het is aan de compliance functie om hier een effectieve *challenge* op uit te voeren. Op deze manier wordt continu en stapsgewijs gebouwd aan een duurzaam compliant organisatie.